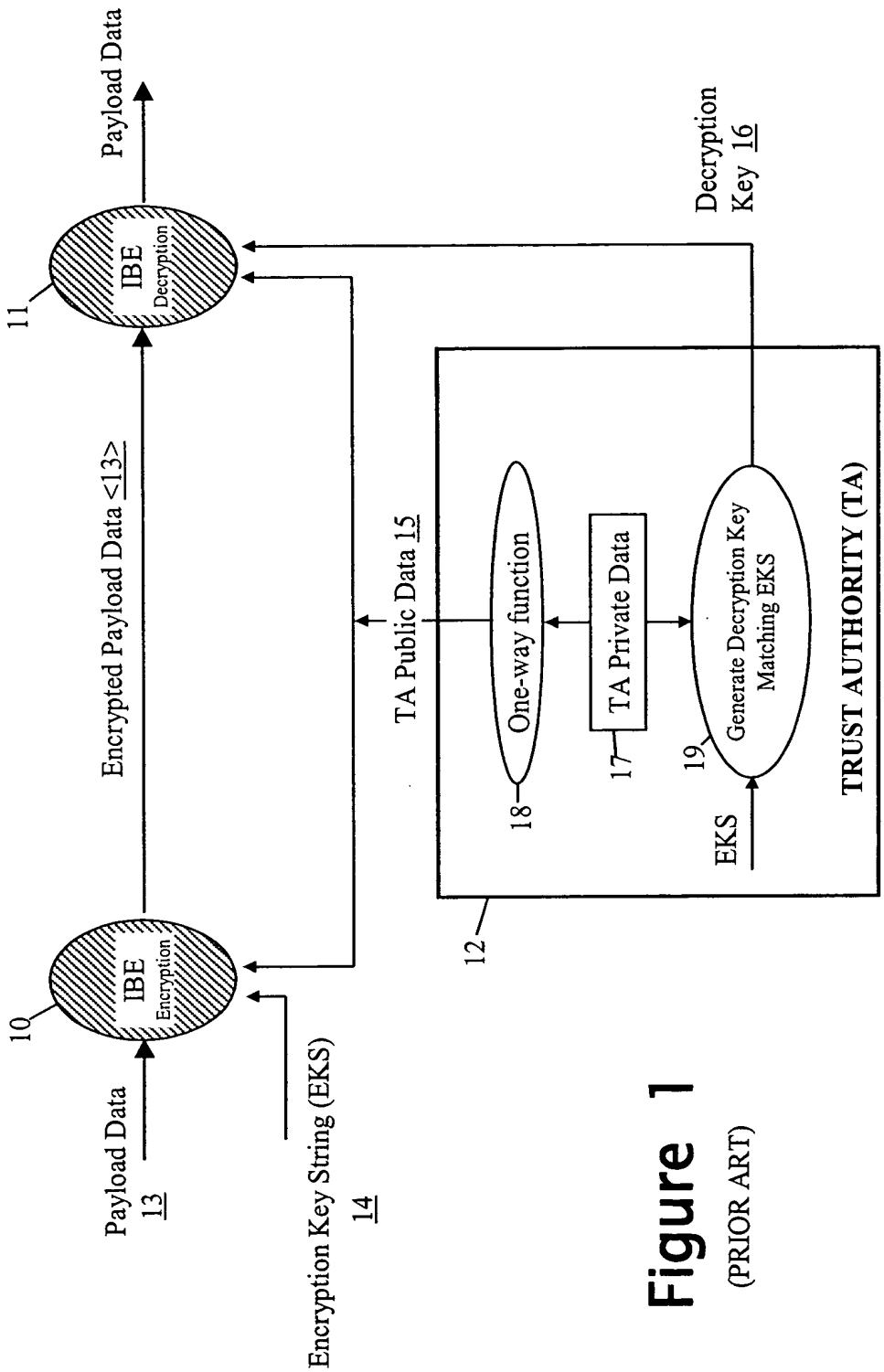
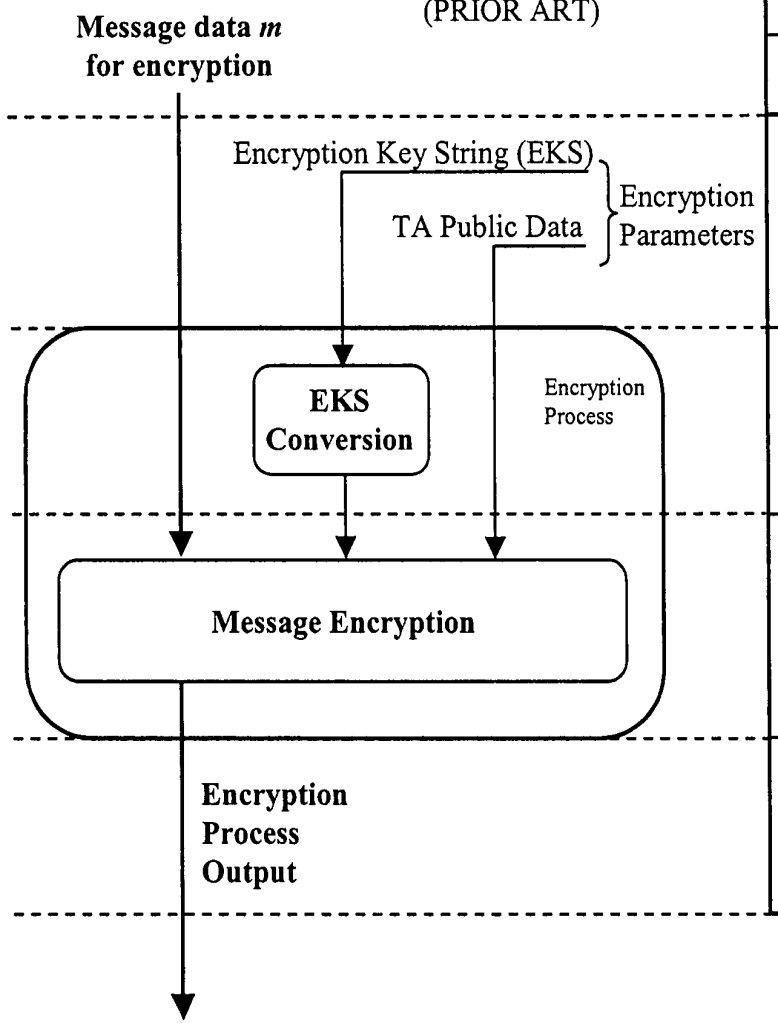


Figure 1
(PRIOR ART)

Figure 2

(PRIOR ART)



Identifier-Based Method		
Quadratic Residuosity	Bilinear Mappings $\hat{p}: G_1 \times G_1 \longrightarrow G_2$	RSA Based
EKS Modulus N	EKS (P, sP) where P is in G_1 s is secret of TA	EKS Modulus n
$K = \#(\text{EKS})$	"Map-to-point" hash $Q_{ID} = H_1(\text{EKS})$ *where* $H_1: \{0,1\}^* \longrightarrow G_1$	e = #(EKS)mod n
For each bit: $s_+ \equiv (t_+ + K/t_+) \bmod N$ $s_- \equiv (t_- - K/t_-) \bmod N$	$V = m \oplus H_2(\hat{p}(sP, rQ_{ID}))$ *where:* $H_2: G_2 \longrightarrow \{0,1\}^*$ r is a random number	$m^e \bmod n$
For each bit: s_+, s_-	$V, U (= rP)$	$m^e \bmod n$
(knowledge of EKS and TA concerned also needs to be available)		

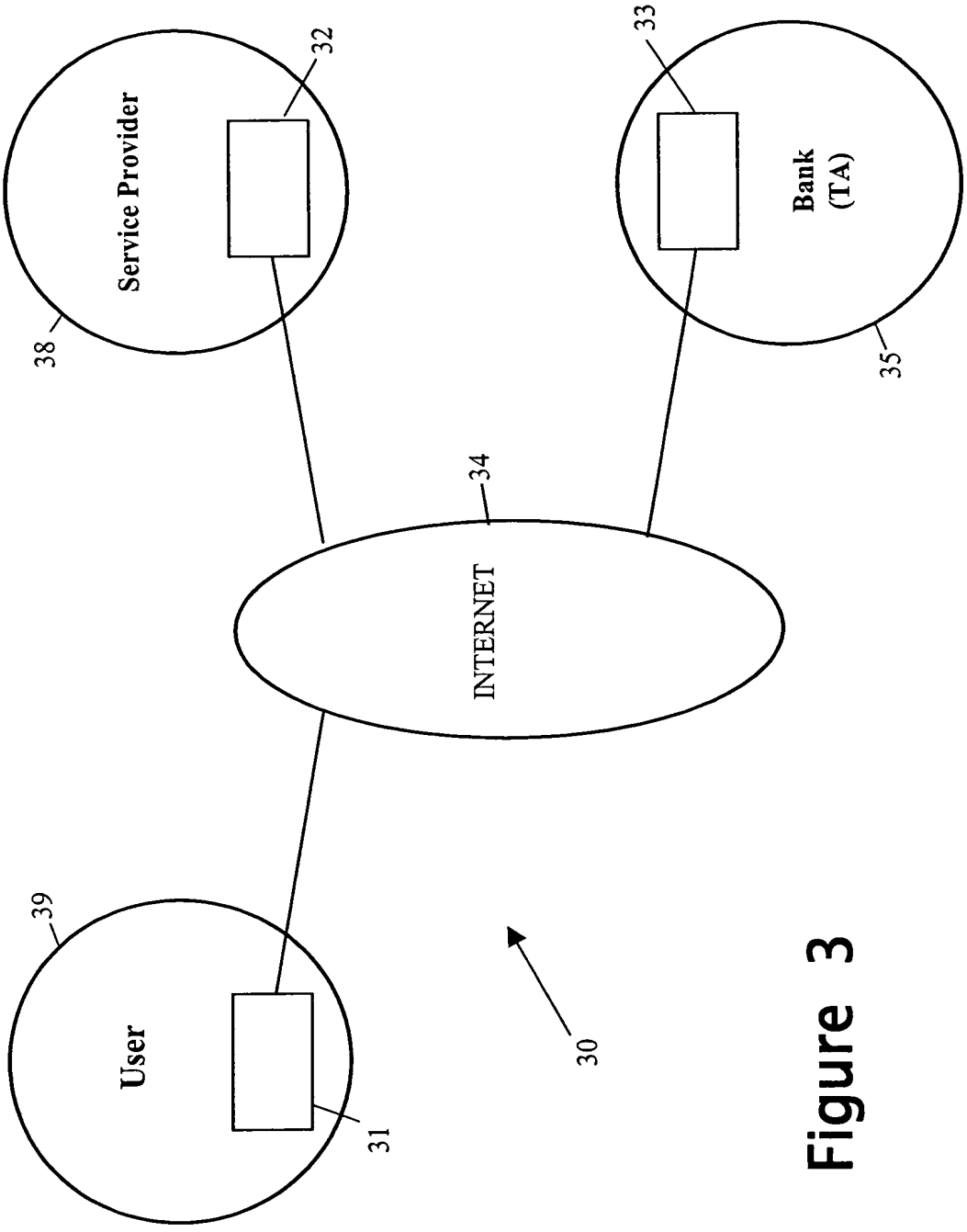


Figure 3

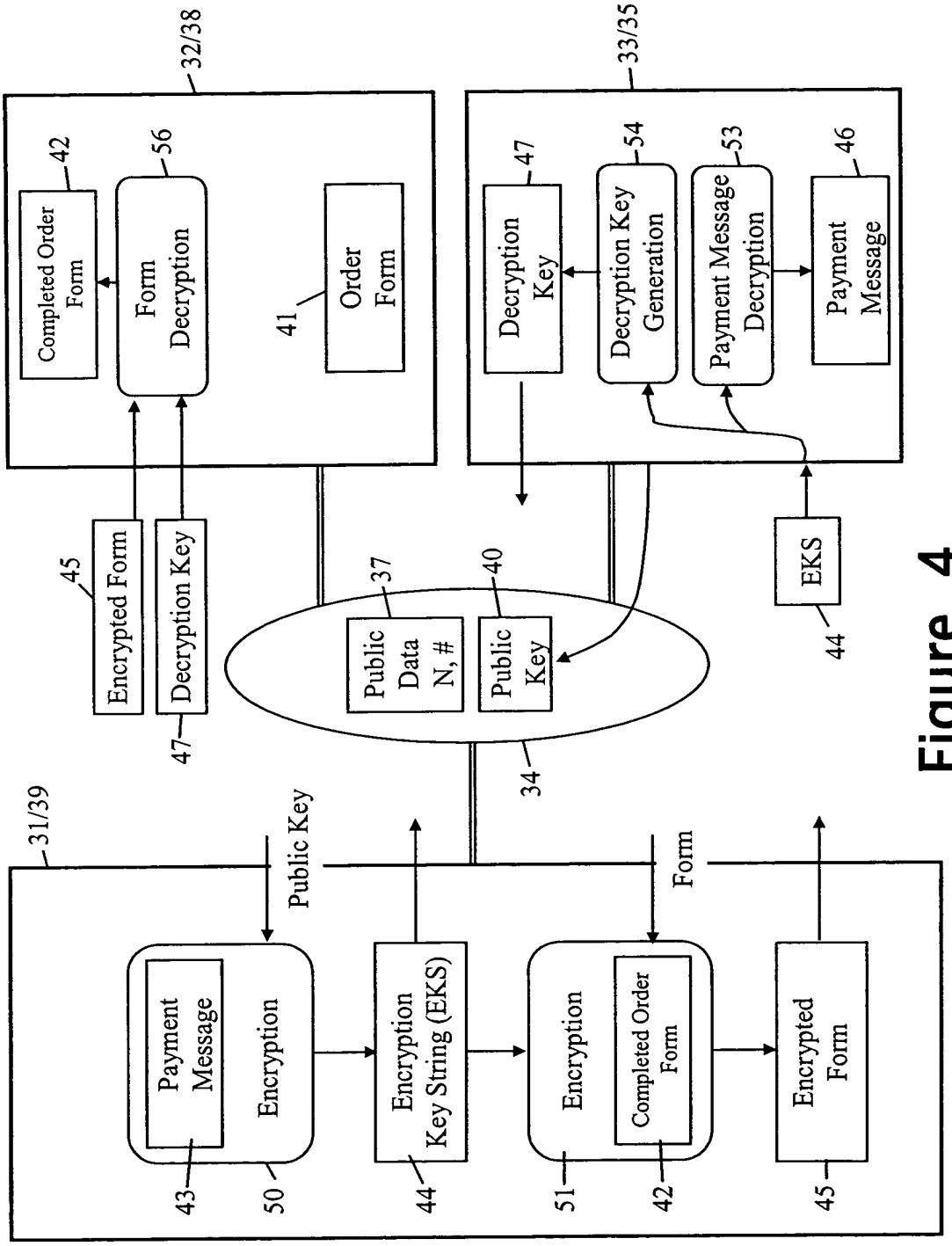

32/38
Completed Order Form
42
Form Decryption
56
Order Form
41
33/35
Decryption Key
47
Decryption Key Generation
54
Payment Message Decryption
53
Payment Message
46
Encrypted Form
45
Decryption Key
47
Public Data N, #
37
Public Key
40
EKS
44
34
31/39
Public Key
Form
Payment Message
Encryption
43
50
Encryption Key String (EKS)
44
Encryption
Completed Order Form
51
42
Encrypted Form
45

Figure 4